AO 91 (Rev. 11/11) Criminal Complaint 24-030

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America
v.

Ruben Filipe Gabriel Martins
a/k/a "Feepsy"

Defendant(s)

Case No. 24-mj-1338

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 6, 2024 in the county of Montgomery in the Eastern District of Pennsylvania, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. 1343	On or about April 6, 2024, Ruben Filipe Gabriel Martins knowingly and intentionally did devise and intend to devise a scheme and artifice to defraud Victim 1, located within the Eastern District of Pennsylvania, of money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, caused to be transmitted by means of wire communication in interstate commerce text messages to Victim 1 on or about April 6, 2024, in violation of Title 18, United States Code, Section 1343.

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

/s/ *Zachary Fuller*
Complainant's signature

Special Agent Zachary Fuller
Printed name and title

Sworn to me telephonically or by other reliable electronic means:

Date: 08/19/2024

Lynne A. Sitarski
Digitally signed by Lynne A. Sitarski
Date: 2024.08.19 16:40:48 -04'00'
Judge's signature

City and state: Philadelphia, Pennsylvania

Honorable Lynne A. Sitarski, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF COMPLAINT AND WARRANT

I, Zachary Fuller, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I submit this affidavit in support of an application for a warrant to arrest RUBEN FILIPE GABRIEL MARTINS, a/k/a "Feepsy" ("MARTINS"), for violation of 18 U.S.C. § 1343 (wire fraud). MARTINS is currently in local custody in Los Angeles, California where he is being held on an arrest warrant issued by the Hon. Thomas Murt, Magisterial District Judge, Montgomery County, Pennsylvania, for receiving stolen property, computer trespass and related offenses. As explained below, there is probable cause to believe that MARTINS used a Google Voice number to send a phishing[1] link to a victim in the Eastern District of Pennsylvania that led to $60,000 worth of cryptocurrency being stolen from the victim's Coinbase account.

2. Since May 2018, I have been a Special Agent with the Philadelphia Federal Bureau of Investigation ("FBI") assigned to the Criminal Cyber Squad and Philadelphia Cyber Task Force. During my employment with FBI, I have conducted numerous criminal cyber investigations involving online communication forums using and exploitation of information technologies. My responsibilities as a member of the Task Force include investigating cybercrimes, seeking and executing arrest and search warrants, monitoring Title III intercepts, and assisting the FBI Cellular Analysis Survey Team ("CAST") in responding to requests submitted by law enforcement agencies. Specifically, I assist CAST with cellular record analysis, technical assistance, and

[1] "Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

mapping, and conducting tracking missions using historical cell site analysis in order to geo-locate target cell phones used by subjects, accomplices, fugitives, witnesses, and/or victims of crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. All dates, times and cryptocurrency figures are approximate.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 1343 has been committed by MARTINS.

PROBABLE CAUSE

Background on the Com

18. I am part of an investigation into a group of cyber-criminal actors who refer to themselves as the Com. The Com consists of a geographically diverse group of individuals, organized in various subgroups, all of whom coordinate through online communication applications such as Discord and Telegram to engage in various types of criminal activity to include corporate intrusions, SIM swapping, cryptocurrency theft, commissioning in real life violence, and Swatting. MARTINS is a member of the Com and has worked with other members on multiple occasions to steal cryptocurrency and launder the stolen funds.

Theft from Victim 1

19. On April 6, 2024, a resident from Towamencin Township (located in the Eastern District of Pennsylvania) ("Victim 1") came to the Towamencin Township Police

Department to report $60,682.57 in cryptocurrency had been stolen from his Coinbase account. Victim 1 advised that on April 5, 2024, in the late evening hours, he received a text from phone number 706-452-1926, purportedly from Yahoo, stating that a phone number change had been made on his Yahoo account and to reply with "N" if it was unauthorized. Victim 1 responded, "N" to the text message.

20. Victim 1 further advised that, shortly thereafter, on April 6, 2024, he received a call from 864-756-1142. The caller claimed he was a representative from Coinbase and advised Victim 1 that his Coinbase account had been compromised. During the call, Victim 1 also received a text message from 818-850-2627 (the "2627 Number") that provided a link to a website "191284-Coinbase.com." Victim 1 could not recall whether he clicked on the link or entered his login credentials. He advised that his username and password were the same for both Yahoo and Coinbase.

21. Based on my training and experience, I am aware that actors engaged in phishing offenses frequently register domains closely resembling the branding and layout of the authentic domain. The use of a hyphen (-) creates a unique domain not affiliated with the actual brand. I know that victims of phishing offenses frequently mistake this for a subdomain, which is frequently used by brands for various functions, including securing accounts.

22. Open-source research of the website "191284-coinbase.com" showed that the domain was registered to "Matthew Cram" from Mattwil, Switzerland. A review of domains shows that this registrant name is connected to 214 domains with similar phishing links.

23. Victim 1 advised that during the phone call with phone number 864-756-1142, he was instructed to provide his Two Factor Authentication (2FA) code from Coinbase to facilitate

a transfer to a secure wallet. Based on my training and experience, I know that Coinbase offers a security setting whereby Coinbase sends a 2FA challenge before authorizing a fund transfer. Believing the caller was from Coinbase, Victim 1 provided the codes as instructed. Victim 1 subsequently realized this was a scam and that his Coinbase account had been drained. At the time of the theft, Victim 1's funds were valued at $60,682.57.

24. Cryptocurrency blockchain tracing showed that Victim 1's stolen funds were subsequently transferred to several cryptocurrency exchange accounts, with the majority of funds being transferred through smart contracts and cryptocurrency mixing services. Additional analysis revealed a portion of the stolen funds were deposited into a Stake.com[2] account that had previously been funded by MARTINS on 27 separate occasions. Records from Stake.com revealed that MARTINS provided the email address feepsy@riseup.net and an Italian Passport with a different name during account registration.

Google Records

25. On May 9, 2024, a Google search warrant for the 2627 Number was issued by the Hon. Thomas Branca, Court of Common Pleas, Pennsylvania. Analysis of the responsive Google records revealed that between April 5 and May 3, 2024, the 2627 Number sent or received text messages to/from 23 unique phone numbers. Approximately 18 of the text messages contained phishing links or outgoing messages which appear to involve phishing attempts.

26. The Google records show that on April 26, 2024, the 2627 Number sent a text message to "AHN Management LLC d/b/a Hermes Bitcoin" ("Hermes Bitcoin") customer service

[2] The website Stake.com is an online gambling service. Based on my training and experience, I know that criminals often use the website to launder cryptocurrency.

at (323) 400-3100 to report a problem with an attempted transaction on April 25, 2024 concerning a Bitcoin Automated Teller Machine (ATM) in Los Angeles, California (the "ATM Transaction").

27. On June 3, 2024, the Hon. Thomas Branca, Court of Common Pleas, Pennsylvania, issued a search warrant for the Hermes Bitcoin records regarding the ATM Transaction. Review of the responsive records revealed MARTINS' Portugal citizen identification card and surveillance images of a male at the ATM, which depict the same individual.

28. The Google records also showed that the 2627 Number is associated with email address Saifalcide859@gmail.com, which is connected by cookies to filipemartins20111@gmail.com (which is a variation of MARTINS' name) and feepsbruh@gmail.com (which is a variation of MARTIN's moniker "Feepsy"). On May 22, 2024, a Google search warrant for the Saifalcide859@gmail.com account was issued by the Hon. Thomas Rogers, Court of Common Pleas, Pennsylvania. The responsive Google records showed that on April 4, May 2, May 3, and May 10, 2024, the Saifalcide859@gmail.com account was accessed from an IP address that resolved to Turriff, United Kingdom.

29. Review of Immigration and Customs Enforcement (ICE) records shows that MARTINS flew from London to Los Angeles on March 7, 2024, and flew back to London on April 2, 2024. MARTINS then flew from London to Los Angeles on April 18, 2024 and flew back to London on April 30, 2024. The images captured by ICE during MARTINS' entries and exits from the United States depicted the same individual shown in the ATM surveillance photos discussed above.

30. The ICE records also showed that upon entry into the United States, MARTINS provided the phone number +447908488576 and the email address feepsy@riseup.net (the same

email address associated with the Stake.com account mentioned above), a home address of 24 High St, Turriff AB53 4EA, United Kingdom (which appears to be a mail delivery service), and local address in the United States of 915 N La Brea Ave, West Hollywood, CA 90038.

31. A review of Google activity logs from the Saifalcide859@gmail.com account showed that an Android device accessed the account on April 5, 2024 at 12:08 A.M. (UTC), approximately 1 day prior to the first phishing text sent to Victim 1. Google recorded the device time zone as British Summer Time (GMT +0100). BST is the time zone for Great Britian, where MARTINS was believed to be, based on his residence and flight records, as set forth above.

CONCLUSION

32. I request that the Court issue an arrest warrant authorizing the Federal Bureau of Investigation or any authorized law enforcement officer to arrest MARTINS.

Respectfully submitted,

/s/ *Zachary Fuller*
ZACHARY FULLER
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me telephonically or by other reliable electronic means on August 19, 2024:

Lynne A. Sitarski
Digitally signed by Lynne A. Sitarski
Date: 2024.08.19 16:41:54 -04'00'

HONORABLE LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE